Math100B - HW #4

Jay Ser

2026.02.08

1.

One can assume $f(x)$ is monic; if $f(x)$ has leading coefficient $a_n \neq 1$, then $\langle f(x) \rangle = \langle \frac{1}{a_n} f(x) \rangle$ as ideals in $\mathbb{R}$ since a_n is a unit in $\mathbb{R}$. Since $f(x)$ has no repeated roots, either

1. $f(x) = (x - a_1)(x - a_2)(x - a_3)$ with $a_1, a_2, a_3 \in \mathbb{R}$ distinct.
2. $f(x) = (x - a)(x^2 + c)$ with $c \in \mathbb{R}_+$.

First, consider case 1. Then the assumption for Question 3 holds, so its result applies:

$$\mathbb{R}[x]/\langle f(x) \rangle \cong \mathbb{R}^3$$

Next, assume case 2. $\langle x^2 + c \rangle$ and $\langle x - a \rangle$ are comaximal: $(x - a)(x + a) = x^2 - a^2 \in \langle x - a \rangle$, and $x^2 + c - (x^2 - a^2) = c + a^2 \neq 0$, so the ideal $\langle x^2 + c \rangle + \langle x - a \rangle$ contains a unit, i.e., $\langle x^2 + c \rangle + \langle x - a \rangle = \mathbb{R}[x]$. By the Chinese Remainder Theorem,

$$\mathbb{R}[x]/\langle x^2 + c \rangle \langle x - a \rangle \cong \mathbb{R}[x]/\langle x^2 + c \rangle \times \mathbb{R}[x]/\langle x - a \rangle$$

By definition, the product of ideals $\langle x^2 + c \rangle \langle x - a \rangle$ is equal to $\langle (x^2 + c)(x - a) \rangle = \langle f(x) \rangle$. Also, it was shown in midterm 1 that $\mathbb{R}[x]/\langle x^2 + c \rangle \cong \mathbb{C}$ and by homework something, $\mathbb{R}[x]/\langle x - a \rangle \cong \mathbb{R}$. Putting all these isomorphisms together,

$$\mathbb{R}[x]/\langle f(x) \rangle \cong \mathbb{C} \times \mathbb{R}$$

2.

(a)

Suppose $(x, y) \in F \times F$ is nilpotent, say $(x, y)^n = 0$ with $n \in \mathbb{Z}_+$. By the definition of the product ring,

$$(x, y)^n = (x^n, y^n) = (0, 0)$$

Through the projection homomorphisms, one sees $x^n = y^n = 0$ in F. But nonzero nilpotent elements are zerodivisors, of which there are none in fields. So $x = y = 0$ in F. This shows that $F \times F$ has no nonzero nilpotent elements.

(b)

$x \notin \langle x^2 \rangle$ because $\mathbb{Q}[x]$ is a Euclidean domain and x is of lower degree than x^2. So $\bar{x} \neq 0$ in $\mathbb{Q}[x]/\langle x^2 \rangle$ and of course $\bar{x}^2 = 0$. So $\bar{x}$ is nilpotent in $\mathbb{Q}[x]/\langle x^2 \rangle$, which means $\mathbb{Q}[x]/\langle x^2 \rangle$ cannot be isomorphic to $\mathbb{Q} \times \mathbb{Q}$.

3.

By the Chinese Remainder Theorem,

$$\varphi : F[x] \to \prod_{i=1}^{n} (F[x]/\langle x - a_i \rangle)\ f(x) \mapsto (f(x) + \langle x - a_1 \rangle, \ldots, f(x) + \langle x - a_n \rangle)$$

is an isomorphism with kernal $\langle x - a_1 \rangle \cap \ldots \cap \langle x - a_n \rangle$. But since the $x - a_i$'s are distinct linear polynomials, the ideals $\langle x - a_i \rangle$ and $\langle x - a_j \rangle$, $i \neq j$, are pairwise comaximal: $x - a_i - (x - a_j) = a_j - a_i \neq 0$, which is a unit because it is a nonzero coefficient over a field, so the ideal $\langle x - a_i \rangle + \langle x - a_j \rangle = F[x]$. So

$$F[x]/(\prod_{i=1}^{n} \langle x - a_i \rangle) \cong \prod_{i=1}^{n} (F[x]/\langle x - a_i \rangle)$$

Additionally, it follows immediately from definition that the product ideal $\langle x - a_i \rangle \langle x - a_j \rangle$ is equivalent to $\langle (x - a_i)(x - a_j) \rangle$. Hence $\prod_{i=1}^{n} \langle x - a_i \rangle = \langle \prod_{i=1}^{k} (x - a_i) \rangle = \langle p(x) \rangle$. Also, it was shown whenever ago that $F[x]/\langle x - c \rangle \cong F$ for any $c \in F \setminus 0$. So

$$F[x]/\langle p(x) \rangle \cong F^n$$

4.

Denote F as the field of fractions of R. For any integer $a \in \mathbb{Z}_{\geq 0}$, let $a = \sum_{i=1}^{a} 1$ in R and F.

Recall that, by the construction of the field of fractions, R embeds itself into F as a subring. Let $n := \text{char} R$. If $n = 0$ as an integer, then $\forall m \in \mathbb{Z}_{\geq 0}$, $m \neq 0$ in R. Thus $m \neq 0$ in F, which means $\text{char} F = 0$ as well. If $n > 0$ as an integer, then $n = 0$ in R, and thus in F. Furthermore, $\forall m \in \mathbb{Z}_{\geq 0}$ where $m < n$, $m \neq 0$ in R. It follows that $m \neq 0$ in F as well, hence $\text{char} F = n$. This shows $\text{char} F = \text{char} R$.

Let $n = \text{char} R = \text{char} F$, and suppose n is not zero and not prime; say $n = ab$, $a, b > 1$. Then $ab \neq 0$ in F. Furthermore, $a, b \neq 0$ in F because $a, b < n$ and n is the characteristic of F. This shows that a is a zerodivisor in F, which contradicts the fact that fields don't have zerodivisors. It follows that the characteristic of an integral domain is 0 or a prime number.

5.

For any $a \in R \setminus 0$, define

$$\varphi : R \to R;\ r \mapsto ar$$

Because R is an integral domain φ is injective:

$$ar = as \iff r = s$$

Because R is finite, injection implies surjection. Finally, by definition of φ, it is clear that $\varphi(R) = \langle a \rangle$. So $\langle a \rangle = R$, which means a is a unit. This shows that every nonzero element of R is a unit; R is a field.

6.

Since F is finite, $\text{char}F \neq 0$. Namely, then, $\text{char}F = p$ for some prime p. Note that $\text{char}F$ is just the order of 1 in the abelian group F^+. So $p \mid |F|$. Take any $x \in R \setminus 0$. Since

$$px = 0x = 0$$

in F, where the integer p is viewed as $\sum_{i=1}^{p} 1$ in F, it follows $\text{o}(x) \mid p$. $x \neq 0$, the identity in the abelian group F^+, so $\text{o}(x) \neq 1$, and p is a prime integer, so $\text{o}(x) = p$. Thus, it is impossible for any prime q other than p to divide the order of F. If q did divide F, then by the Cauchy theorem, $\exists y \in F^+$ such that $\text{o}(y) = q$, which is a contradiction.

7.

Here's a helpful lemma:

Lemma. *Suppose R is a principal ideal domain. Then $p \in R$ is irreducible $\iff$ p is prime.*

Proof of Lemma. In any integral domain, prime $\implies$ irreducible: if $p = ab$ and p is prime, $p \mid a$ or $p \mid b$. But $a \mid p$ and $b \mid p$, so p is associate with a or b. In other words, the only elements that divide p are its associates and units, which means p is irreducible.

Next, suppose $p \in R$ is irreducible and $p = ab$. It must be shown that if $p \nmid a$, then $p \mid b$. Consider the ideal $\langle p, a \rangle$. Because R is a PID, $\exists d \in R$ such that $\langle d \rangle = \langle p, a \rangle$. But by assumption on p and a, the only elements that divides both p and a are units. Hence we can take $d = 1$, then $\exists r, s \in R$ such that $rp + sa = 1$. Multiplying both sides by b,

$$rbp + sab = b$$

p divides the left side of this equation, so $p \mid b$ as well. This shows p is prime. $\square$

It was already shown in class that $F[x]$ is a Euclidean Domain (we showed that a Euclidean algorithm exists for $F[x]$). We then proved in the midterm that $F[x]$ is in fact a principal ideal domain (namely, we showed that a greatest common denominator exists for any two elements $f(x), g(x) \in F[x]$). Thus the lemma above applies and can be used to solve the problem.

Given any $\varphi : F[x] \to R$, where R is an integral domain,

$$F[x]/\ker\varphi \cong \varphi(R)$$

by the first isomorphism theorem. But because R is an integral domain, its subrings, and thus ideals, are integral domains as well. So $F[x]/\ker\varphi$ is an integral domain, which means $\ker\varphi$ is a prime ideal. 0 is a prime ideal, so $\ker\varphi$ could be the zero ideal or a nonzero prime ideal. Suppose $\ker\varphi$ is not the zero ideal. Since $F[x]$ is a PID, let $\ker\varphi = \langle p(x) \rangle$. A principal ideal is prime $\iff$ its generator is a prime element. But by the lemma above, prime elements are irreducible elements. Irreducible elements generate maximal ideals in PIDs (namely, we showed that irreducible elements of $F[x]$, i.e., the irreducible polynomials, generate max ideals in $F[x]$), so $\ker\varphi$ must be a maximal ideal in $F[x]$.

8.

(a)

Recall that the binomial theorem holds in any commutative ring:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

where $\binom{n}{k}$ as an element of R is the sum of the identity $\binom{n}{k}$ times.

Take $a, b \in \operatorname{rad} I$. Suppose $a^n \in I$ and $b^m \in I$ for $n, m \in \mathbb{Z}_+$. For any $r \in R$, $(ra)^n = r^n a^n \in I$, so $\operatorname{rad} I$ is closed under scalar multiplication. To see it is closed under addition as well, consider

$$(a+b)^{m+n} = \sum_{k=0}^{m+n} a^k b^{m+n-k}$$

In each of the summand, either $k > n$ or $m + n - k > m$, so at least one of a^k and b^{m+n-k} is in I and thus the entire term. Since each summand is in I, the sum is in I as well. $(a+b)^{m+n} \in I$, so $a + b \in \operatorname{rad} I$. This shows that $\operatorname{rad} I$ is an ideal.

(b)

Let I be a prime ideal. By definition, $I \subset \operatorname{rad} I$. Next, take any $a \in \operatorname{rad} I$ with $a^n \in I$. $a^n = a^{n-1}a \in I$ and I is prime, so either $a \in I$ or a^{n-1}. If the former, there is nothing more to be shown. If the latter, $a^{n-1} = a^{n-2}a \in I$, so $a^{n-2} \in I$ or $a \in I$. If the latter, there is nothing more to be shown. If the former, then one can continue reducing the exponent of a until either $a \in I$ or $a^2 \in I$. If $a^2 \in I$, then clearly $a \in I$.

(c)

The statement is equivalent to showing

$$\forall P \in \operatorname{Spec} R,\ \operatorname{rad} 0 \subset P$$

Take arbitrary $P \in \operatorname{Spec} R$ and $a \in \operatorname{rad} 0$ with $a^n = 0$. $a^n = 0 \in P$, so by similar reasoning as (b), $a \in P$. This shows $\operatorname{rad} 0 \subset P$.